Blocking Reader: Design and Implementation of a Low-Cost Passive UHF RFID Blocking Reader

Gaurov Narayanaswamy
Department of Electrical Engineering
University of Texas Arlington
Arlington, Texas 76010
Email: gaurov.narayanaswamy@mavs.uta.edu

Shesh Kumar Jagannatha
Department of Electrical Engineering
University of Texas Arlington
Arlington, Texas 76010
Email: sheshkumarj@gmail.com

Daniel W. Engels
Revere Security
4500 Westgrove Drive
Addison, Texas 75001
Email: dwe@alum.mit.edu

***Abstract*—In this paper, we present the *Blocking Reader,* a low-cost privacy protection device that prevents unauthorized reading of RFID tags. The promiscuous nature of the 18000-6C RFID tags poses a threat to personal security and privacy. Privately owned tags on a person can be read by all nearby readers without that person's consent or knowledge, thereby, violating that person's privacy. A low cost privacy protection device, the Blocking Reader, worn on a person's body can be used to prevent these unauthorized tag reads, preserving your privacy. Our low-cost Blocking Reader has been implemented based upon the Chipcon CC1101 chip, and we have characterized its basic read and privacy preserving performance. Using a monopole antenna, the Blocking Reader prevents unauthorized tag reads within 1m of it. Furthermore, when worn on a person's body, the Blocking Reader operates effectively as a privacy preserving device, preventing all nearby readers from reading tags located on or in close proximity to your body.**

I. Introduction

The promiscuous nature of radio frequency identification (RFID) tags implemented in compliance with the ISO 18000-6C protocol is known to be a potential source of security and privacy violations. In this paper, we present the Blocking Reader, a low-cost privacy preserving device that takes advantage of the physics of radio frequency (RF) radiation and the ISO 18000-6C protocol to prevent unauthorized readers from violating your privacy. The Blocking Reader is designed similar to a low-cost ISO 18000-6C compliant reader, but its primary purpose is to legally prevent other readers from reading tags in its vicinity. The Blocking Reader communicates with nearby tags, capturing them and preventing other readers in the vicinity to communicate with them.

A typical RFID system is shown in Figure 1. In this system, the reader is connected to the backend information system and communicates wirelessly with the tags in its interrogation zone. RFID technologies are widely deployed in our everyday lives, and they are becoming even more ubiquitous day by day [5], [3]. Because of their ubiquitous and promiscuous nature, deployed RFID technologies pose significant security and privacy concerns for individuals since the promiscuous technologies allow unauthorized readers to read the tags' identities without the owners knowledge or consent [17], [15]. This means that a person may be easily tracked without their knowledge or their consent. Consequently, security and privacy are important issues in the deployment and continued adoption of RFID systems. Low cost RFID readers will enable the widely anticipated benefits of RFID systems, and they will be the source of security protecting our privacy as we wander through this ubiquitously connected world of ours.

The importance of securing RFID systems has led to a significant number of security and privacy preserving mechanisms to be proposed in the literature. In [18] Weis et.al. presented one of the first papers on the security and privacy problems facing the use of modern RFID systems. The vast majority of these problems arise due to the limited functional capabilities of the RFID tags. Surprisingly, the vast majority of security mechanisms that have been proposed are tag-centric in the sense that they rely upon on-tag mechanisms to secure data and protect privacy. Ari Juels presents a comprehensive survey of these proposed mechanisms in his 2006 survey paper [11]. Mechanisms proposed since this paper's publication are similar in their tag-centric approach.

One of the few security device solutions proposed that does not require on-tag mechanisms or support is the Blocker Tag [13]. The Blocker Tag does take a tag-centric approach in

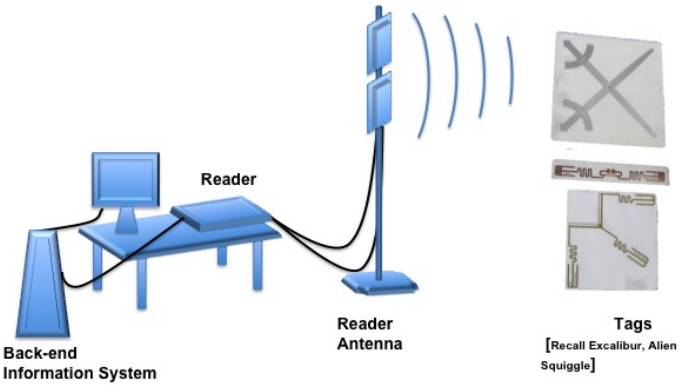

Fig. 1. A Typical RFID System

978-1-4244-5743-4/10/$26.00 ©2010 IEEE

that it attempts to prevent tag reads by responding to all reader communications as if it were a tag. While this approach may thwart some read attempts, its communications collisions may be overcome with simple reader design modifications.

The promiscuity of RFID tags is not unique; magnetic stripe cards, for example, are promiscuous, but we assume that the owner of the card takes the physical responsibility of preventing unauthorized users from physically accessing the card [16]. It is possible to access the information of the tag by any unauthorized reader. Even if tag contents are protected, individuals may be tracked through predictable tag responses; essentially a traffic analysis attack violating location privacy. Spoofing of tags may aid thieves or spies. Saboteurs could threaten the security of systems dependent on RFID technology through denial of service [21]. Technology is advancing at a fast pace. The need for tagging all the products for having good supply chain management and safety is increasing. RFID has promised to provide operational and safety improvements at a very low cost. But what are the risks of this? In case of military it is very important to preserve the privacy of all its operations. The enhanced supply chain visibility that makes RFID so attractive to industry can also, in another guise, betray competitive intelligence [11]. It is a national risk for the military if the enemy forces are monitoring them. The RFID technology has gained popularity in the supply chain industry making the products visible at real time. But there is a threat to the company if other companies can also get this information. We have already discussed how easy it is to get this information. So it is very important to ensure the privacy by making the RFID systems more secure. In this paper we present how we can improve the security and privacy of an RFID system with other devices outside the basic RFID system.

The remainder of the paper is organized as follows. In Section II we review related work to protecting privacy. In Section III we review the portions of the ISO 18000-6C protocol that are relevant to the proper functioning of the Blocking Reader, and in Section IV we review the electromagnetic physics and tag operational characteristics that enable the Blocking Reader to provide security and privacy. The Blocking Reader design is presented in Section V. It's performance is presented in Section VI. Finally, we draw the relevant conclusions in Section VII.

II. Related Work

A significant number of approaches have been proposed to prevent the unauthorized reading of RFID tags. Many of these approaches are physical, some are logical and some electronic. We review several of these proposed privacy protection approaches in this section.

A. Faraday Cage Approach

Metal is known to reflect any RF radiations of certain frequencies [22], [4], [6]. Indeed this can be used to advantage by caging the tags in a container made of metal or metalized foil. We already know that some petty thieves use foil-lined bags for shoplifting. RFID credit cards are prone to digital pick pocketing. Foil lined wallets are sold in the market at a starting cost of $19.85 (via SkyMall.com). The US government is switching to RFID enabled passport card and Enhanced Driver's License (EDL), presents a privacy nightmare. Faraday's cage approach provides a physical protections, but it has physical damaged barriers problems. The physical shields provided by sleeves are easily misplaced or damaged thereby eliminating or reducing their effectiveness.

B. Blocker Tag

Juels et. al. proposed a simple blocker-tag scheme for privacy protection [13]. Here blocker tags selectively exploit the tree walking singulation protocol. Indeed his approach was to participate in the tag communication in a non-compliant way causing active jamming. Here the the approach is behaving like a tag and sending a full spectrum of serial numbers. Hence this process will obscure the serial numbers of other tags. This makes readers hard to singulate tags in the field. The blocker tag when carried by a person induces a physical region of privacy protection around the person. A passive blocker tag's workability limited because of multi-path hot spots and week spots. Also, narrow beam reader antennas,such as high gain or curtain antennas isolate blocker tags from other tags.

C. Killer Tag approach

This is a decent approach to consumer privacy, the tags are killed with the `Kill` command whenever necessary as proposed by the AutoID Center[16], [9]. In the RFID world, all manufactured products are tagged with a unique RFID tag to keep track of products and its identity. When the products are sold to the consumer, it can be simply killed with a simple `Kill` command. Indeed this approach is inadequate, the killed tags can't be used. In many RFID applications require tags to still be active, once killed tags cannot be activated. This approach is already used in practice. There is no cost as such to kill a tag, but this is a compulsive approach similar to tampering the tag. Many retailers don't want to manage passwords and kill at point of sale. It is bad for reverse logistics.

D. Active Jamming approach

Radio jamming is another physical means to block tags by actively broadcasting high power signals to decrease the signal to noise ratio received by either the tag or the reader. Tag jamming creates a noise shield around the tag. In this approach an illegal broadcast of high power RF signals are done to create disturbance in communication. Hence having a Jamming effect. Unlike the blocker tag which is designed to be FCC compliant, active jamming requires a license to operate. Active jamming is already in practice in jails where they want to jam any cell phone signals. Jamming was also used in World War II, and every conflict since, to prevent enemies from communicating. But active jamming is simply illegal for most persons.

E. Smart RFID Tag approach

RFID tags can become smarter by implementing additional features on top or in the protocol making it secure. Many concepts are being proposed by S.A. Weis in his paper and thesis [18], [20].

1) Hash-Lock approach: In this approach [18], [20] the tag are locked and refuses to give its ID unless unlocked. The unlock code being a meta-ID is only known to a authorized reader. Hence the privacy of the tags are preserved even after tagged products sold to other customers. The meta-ID can be shared between readers authorizing them to read. But how secure is this approach, snooping can retrieve the Tag ID when communicating with a authorized reader. Also Meta-ID can be cracked. It also creates inconvenience for the consumer to handle this.

2) Re-encryption approach: Re-encryption approach proposed by Juels and Pappu [12]. It was mainly focused on financial cryptography. The RFID tagged bank notes are prone to privacy and security issues. The serial numbers of the tags are encrypted with law-enforcement public key. Periodic re-encryption is done to avoid guessing of different appearances. The main drawback of this is the cost of implementation, difficult to re-encrypt every time.

3) Silent Tree-Walking approach: The Silent Tree-Walking approach was proposed by S.A.Weis [18]. This concept was proposed mainly to avoid the threat posed by passive eavesdroppers. By encrypting the reader communication it is possible to avoid passive eavesdroppers to infer the Tag ID. But this approach is not suitable if another active reader is trying to communicate with the tag.

So none of these approaches suitably preserve the privacy for personal tags. As we explained smart tags don't work for a variety of reasons. These approaches are suitable only for specific applications. But the concept of Blocker Tag is exploited and instead of behaving like a tag, the Blocking Reader behaves like a reader. The Blocking Reader uses compliant ways to achieve blocking, again inducing a physical region of privacy.

III. ISO 180006-C GENERATION-2 PROTOCOL

The ISO 18000-6C protocol was originally developed under the Auto-ID Center and completed under EPC Global [9] before submission to ISO. This is the standard for passive UHF RFID systems for communication at 860MHz-960MHz with an effective identification range of 5-10m. The protocol has commands that are used to establish communications between reader and tag. The interrogator modulates the carrier wave 902MHz-928MHz and the following commands are sent. Based on the commands sent the passive RFID tag will backscatter and sends commands by further modulating. The UHF band is separated into various regions around the world. In Europe it is from 865MHz-868MHz with 200KHz channels, whereas in United States and Canada it is 902MHz-928MHz with 500KHz channel. In this paper we consider just the US range, but the analysis works for any specific region's frequency range.

The reader to tag communication uses DSB-ASK, SSBASK, or PR-ASK modulation. The reader modulates the RF carrier signal in one of the above mentioned modulation schemes with PIE encoding to communicate with the tag. The tag to reader communication also uses the same modulation scheme as mentioned above but the backscattered data shall be encoded by FM0 baseband or Miller modulation schemes.

The tag identification procedure begins with an inventory round in this protocol. An inventory round consists of Query command which initiates the round. The Query command includes the Q ranging between 0 and 15, DR and M values using which the tag sets its data rate and other parameters. Upon receiving a query a tag shall preload a value between 0 and $2^Q - 1$ into its slot counter. Tags in the Arbitrate state decrement their slot counter every time they receive a QueryRep with matching session thus transitioning to reply state and backscattering an RN16 when their slot counter reached 0000_h. Tags whose slot counter reached 0000_h, who replied and who were not acknowledged shall return to the arbitrate state with a slot number of 0000_h and shall decrement this slot value to $7FFF_h$ at the next Queryrep. The slot counter begins counting again thereby effectively preventing subsequent replies until the tag loads a new random value into its counter [9].

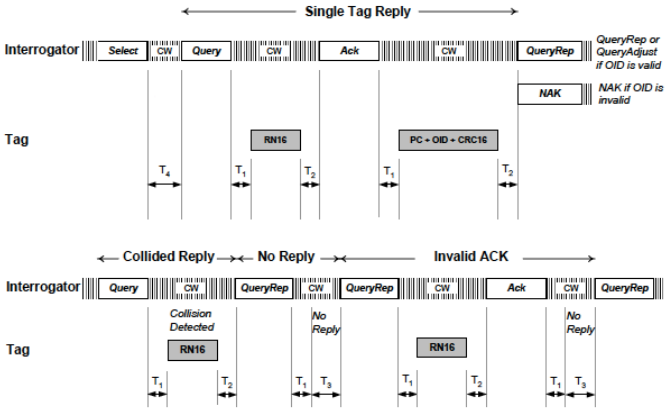

Fig. 2. Link timing [9]

The tags provide 4 sessions (S0, S1, S2 and S3). Tags can be in one and only one session during an inventory round. Two or more readers can use sessions to independently inventory a common tag population. Tags shall maintain an independent inventoried flag for each session. Tags participating in inventory round in one session shall neither use or modify the inventoried flag for a different session.

The reader can stop at any time in the inventory round and it is not compulsory for it to complete the read sequence. Keeping this idea in mind the Blocker Reader repeatedly issues the Query command which will cause the tags to initiate an inventory round repeatedly. This means that tags will next respond to ACK commands and Query commands only. The probability of another reader issuing a correctly timed ACK that is issued before the Blocking Reader's next Query, with

the correct RN16 is extremely low or nearly impossible. Also, by Querying as fast as possible, there is not sufficient time for a complete ACK or Query command from another reader to be finished before the Blocking Reader issues its next Query. This insures that the commands will collide with the commands issued by the Blocking Reader; thus, confusing the tags.

IV. Tag Capture

A. Inside a Passive RFID Tag

A passive UHF RFID tag has no battery to power its functionality. It harvests energy from the carrier wave power from the reader to energize the circuitry and communicate the encoded ID. So the tags reply at the same frequency as the reader. Tag antennae are hence designed to be wide-band in 860-960MHz, but more than just a proper antenna design is required for a properly performing tag [14], [7]. Tags whose operation is solely within the United States will typically have their antenna tuned to have maximum gain at center frequency 915MHz.

Tags are wide-band receivers, it is important for a tag to identify at the frequency slot. In case of multiple reader environment tags receive many signals in the frequency band 902-928MHz. Readers continuously does frequency hopping looking for which slot the tags reply. Tags follow a simple technique to choose which reader to reply to. The tag just identifies the maximum power signal and chooses to reply in that channel. The tag rectifies the incoming signal and detects edges in the power envelope. The sensitivity of the tag is dependent upon how small the high to low thresholds are, and how well it is able to ignore the spurious signals caused by secondary weak reader signals. This is done simply to avoid collisions, it starts replying in this selected slot and other readers are not communicated with. It is quite obvious to note that now the tags have locked to this frequency slot and continues to communicate with this reader provided the reader maintains the same slot and power level. This may be due to filter capacitors and inductors maintaining the charge and hence filter parameters. This is a *Tag Capture* condition. But FCC part 15 regulations allow the reader to stay in the slot for a maximum of 400ms. Hence it depends on the reader frequency hopping, power ramping etc.

B. Reader Physics

In this section we discuss about the communication physics of the reader pertaining to the tag capture mentioned in previous section. The reader complies under FCC part 15.247 for digital modulation systems. Maximum allowable output power is 1W(+30 dBm). Also average time of occupancy on any frequency shall not be greater that 0.4s within a 20s period. Also for frequency hopping if the 20dB bandwidth of the hopping channel is less than 250kHz, the reader shall use at least 50 hopping frequencies. Maximum allowed 20dB bandwidth of the hopping channel is 500kHz.

In practice readers follow techniques that can provide maximum readability, maximum range and avoid collisions [19]. Readers might follow slot occupancy as show in the Figure 3. Here slots refers to the frequency slots occupied during hopping. Freq 1-4 represents different instances of frequency hopping. Typically the slot occupancy time might vary from 300ms to 20ms. Readers spending more time in a slot simply means that reader is reading the tag continuously in this slot period. Since the readability of a tag depends on the slot occupancy time, we can say that the tag capture also depends on the slot occupancy time. During frequency hopping the reader take time in moving to different slot. This may be due to processing time or the transceiver frequency hopping limitations. Sometime it would be necessary to increase the power when a reader doesn't detect any tags in the previous slot. It takes time for processor of the reader to make necessary changes in power. Due to all these reasons there might be a slight delay for the next slot to start. This might be sufficient for other readers to capture the tag.

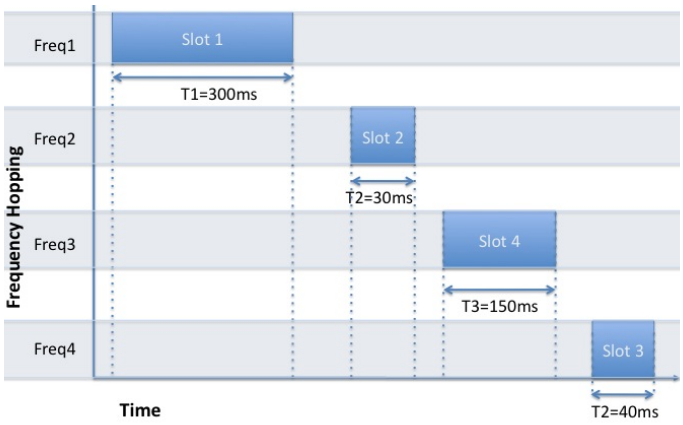

Fig. 3. Reader frequency hopping and slot occupancy

V. Blocking Reader

A Blocking Reader is a reader that prevents other unauthorized readers from communicating with your tags thereby providing security and privacy to its user. The Blocking Reader is an external device that can be used in the vicinity of the RFID system and provides the security as illustrated in Figure 4. Hence, it doesn't require any reconfiguration of the RFID system. The blocking is achieved for a very good range of about 1m with a monopole antenna transmitting at 19-20dBm of power. Any tags inside this range is blocked from other readers trying to access the information of these tags.

A. Low-Cost Reader Design

The Blocking Reader uses the Low-Cost Reader design with low cost components. List of parts and total cost of the design is shown in Table I. PIC C8051F320 provided a very good processing power with a 16Kbyte flash and 25MHz clock. The radio CC1101 [10] is very powerful chip with easy to program packet handling and data rate. Flexible ASK shaping, suitable frequency hopping and programmable power up to +10dBm

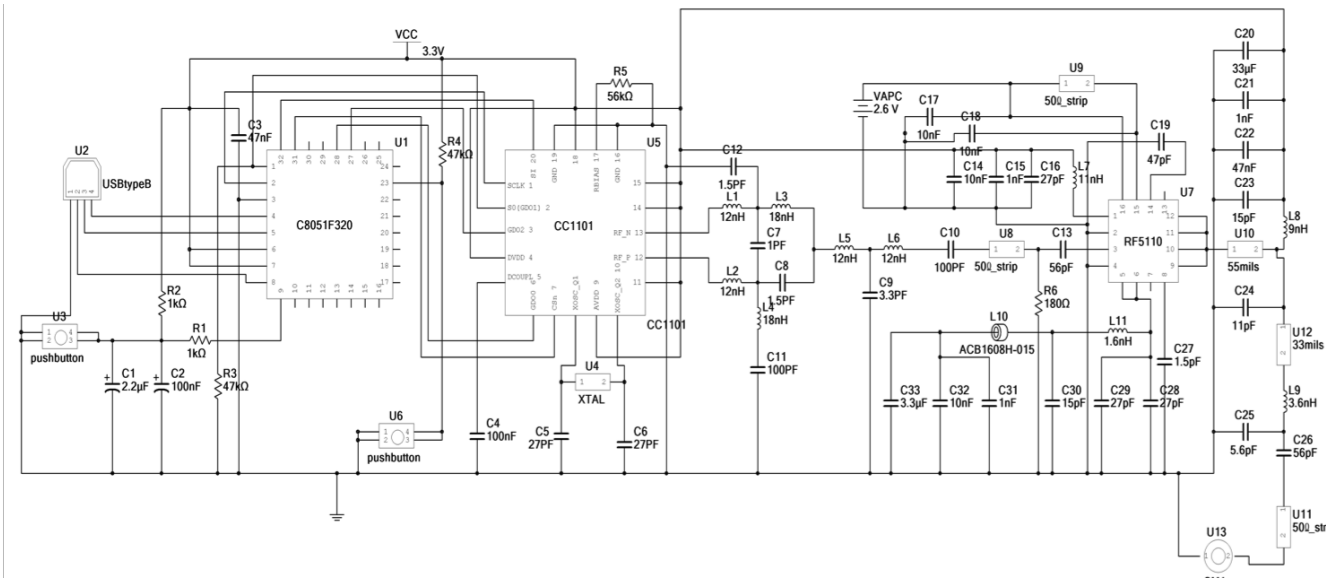

Fig. 5. Complete circuit diagram of Blocking Reader

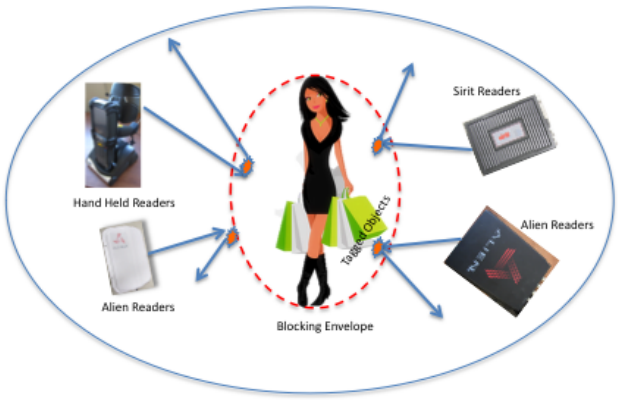

Fig. 4. Blocking envelope around the person.

provided with a optimum blocking range. Amplifier RF5110 is a low cost chip providing amplification of power to improve the blocking range.The complete circuit diagram is as shown in Figure 5. Schematic designed in National Instruments Multisim 10.2. Complete Blocking Reader implementation is estimated to be less than $32 as shown in Table I.

TABLE I
LIST OF PARTS AND COST FOR SINGLE PROCESSOR TRANSCEIVER DESIGN

Components	Type of IC/CKT	Cost($)
Processor	C8051F320	3.16
Transceiver	CC1101	2.55
Antenna (Monopole)	509-ANT-915-06A	7.0
Matching CKT	Discrete Balun and Components	4
Board and other miscellaneous	2 Layer PCB	15
Total Cost		**31.71**

B. 18000-6C Blocking Usage

The Blocking Reader uses the inventory process of the ISO 18000-6C protocol to its advantage. The Blocking Reader transmits a series of `Query` commands that capture the tags. The tags reply to the query with an RN16 value but instead of acknowledging the tag, the Blocking Reader transmit another `Query` command. Now the tag assumes that the reader has not received the RN16. So it sends the RN16 again. This is done continuously to maintain the capturing of the tag. The Blocking Reader uses a low-cost reader architecture design. We present a low-cost reader architectures and implemented the Blocking Reader in the simplest low-cost reader design.

Figure 6 shows the timings of Blocking Reader to tag communication. The Blocking Reader sends a `Query` command every 1.4ms. `Query` commands are 0.8ms in length and the Blocking Reader follows the command by sending a carrier

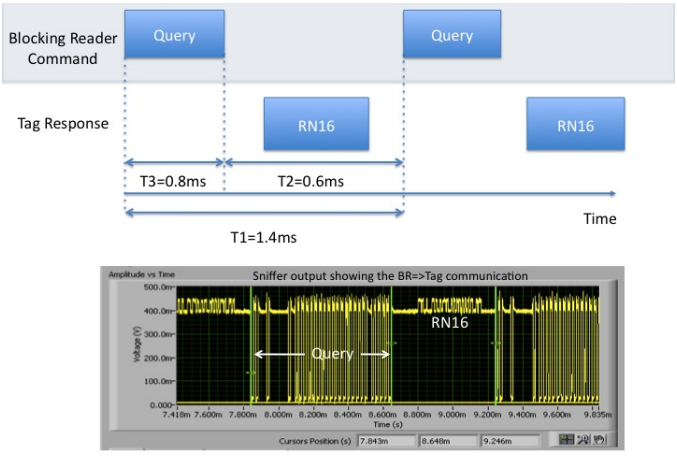

Fig. 6. Tag Response as shown by Sniffer showing the timings.

wave for 0.6ms. In this time, the tag has ample time to respond to the `Query` command sent by the Blocking Reader.

VI. Performance

Several laboratory experiments were performed to determine the performance of the Blocking Reader. In this section, we present the experiments and the significant results from them.

A. Blocking

The Blocking Experiment was designed to determine the maximum distance between a tag and the Blocking Reader at which the Blocking Reader can prevent a reader from reading the tag. Figure 7 illustrates the setup for experiment 1, where the Blocking Reader is rotated around the stationary tag. Figure 8 illustrates the setup for experiment 2, where the tag is rotated around the stationary Blocking Reader.

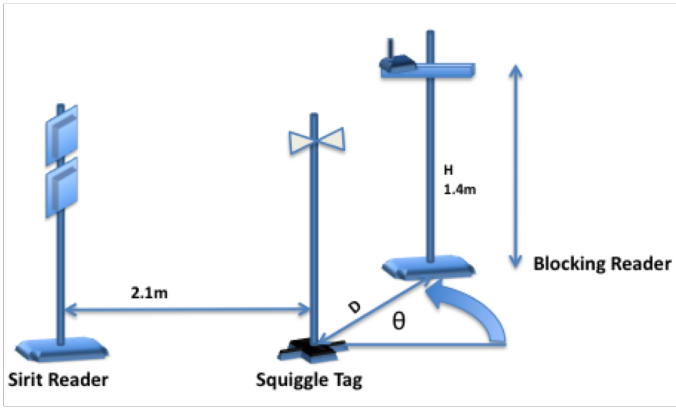

Fig. 7. Configuration of Experimental Setup 1.

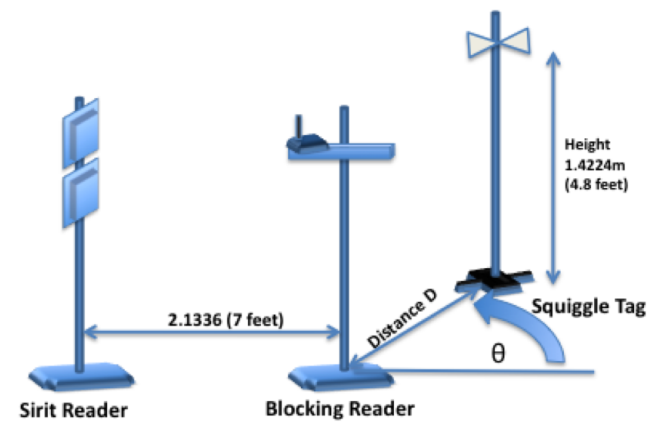

Fig. 8. Configuration of Experimental Setup 2.

The setup for both experiments consists of a Sirit 501 reader that is 2.1m away from the stationary tag (experiment 1) or the stationary Blocking Reader (experiment 2). An Alien squiggle tag is used as a personal tag to be protected from the Sirit reader. The Blocking Reader, Sirit reader and the tag are placed as shown in Figure 7 for experiment 1 and Figure 8 for experiment 2.

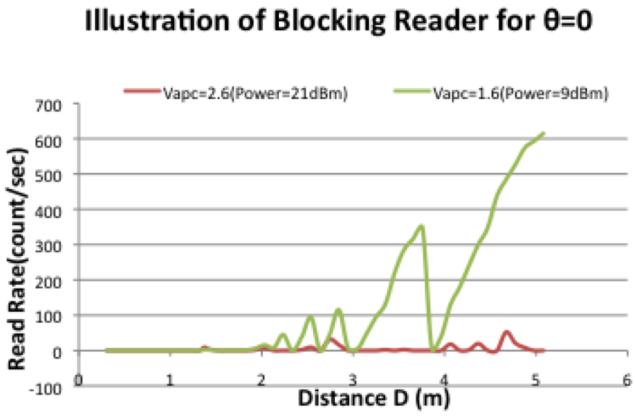

Fig. 9. Results for Setup 1 of Read Rate vs Distance for $\theta = 0$

The power transmitted by the Blocking Reader monopole antenna is varied for different experimental runs of both experiments. Figure 9 shows the results for two different Blocking Reader transmit powers, +21dBm and +9dBm, for experiment 1. The Blocking Reader is switched on in the vicinity of the tag and the read rate of the Sirit Reader is noted. Results are plotted with with the read rate versus the distance between the Blocking Reader and the tag. The Blocking Reader prevents the Sirit reader from reading the tag when it is within 1m of the tag. At approximately 2.1m from the tag, the Sirit reader and the Blocking Reader are equidistant from the tag, yet the read rate is effectively zero for the Sirit reader even for a radiation of 9dBm. This demonstrates the successful use of the `Query` command by the Blocking Reader since at this distance the power at the tag from the Blocking Reader is less than that received from the Sirit reader. Figure 10 shows the read rate plotted with respect to the distance for experiment 2. It shows zero read rate when the Blocking Reader is close to the tag.

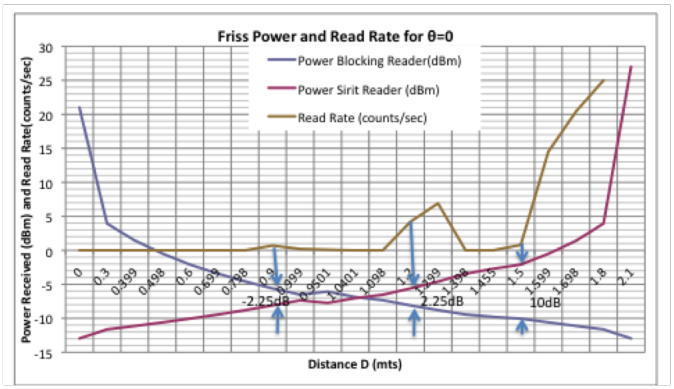

Fig. 10. Read Rate vs Distance for $\theta = 0$, Setup 2.

The blocking envelope is the maximum blocking distance

noted around the stationary tag or the stationary Blocking Reader in the respective experiments. Figure 11 shows the blocking envelope for the stationary tag of experiment 1. Figure 12 shows teh blocking envelope for the stationary Blocking Reader of experiment 2.

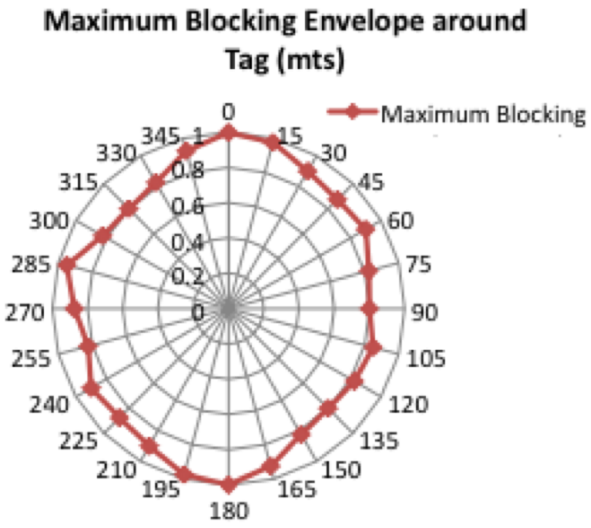

Fig. 11. Blocking Envelope Around Tag

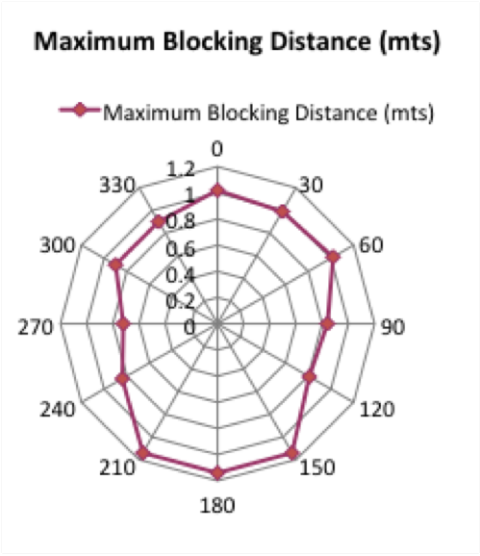

Fig. 12. Blocking Envelope.

B. Human Body Application

In this section we show one practical application of the Blocking Reader. UHF systems behave differently around the human body [1]. In this application, the Blocking Reader is strapped to a person's body and experiments are done to determine the blocking envelope around the person. Figure 13 shows the basic experimental setup used to determine the blocking envelope. The Blocking Reader is placed next to the person at chest height. The person, the tag, and the Sirit reader are all stationary while the Blocking Reader is rotated around the person.

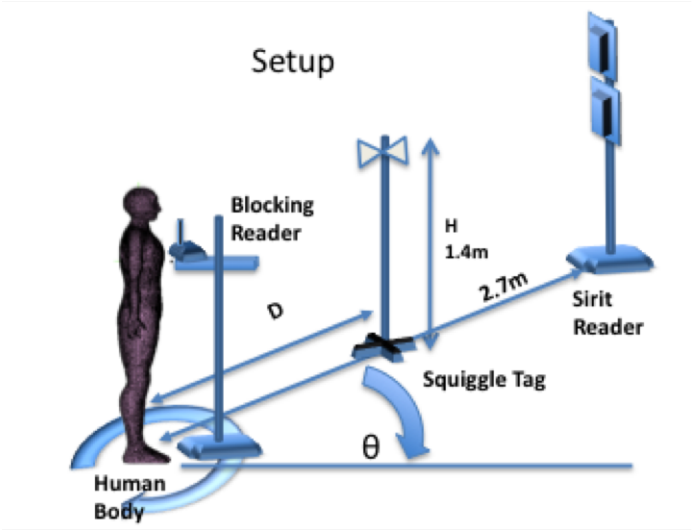

Fig. 13. Experimental Setup for Blocking Around Human Body

Figure 14 shows the results of the blocking envelope experiment with a person. The experiment shows that the person clearly impairs the performance of the Blocking Reader when the person is between the Blocking Reader and the tag. This suggests that a person concerned with their privacy may desire to have two or more blocking readers on their body to ensure complete blocking coverage.

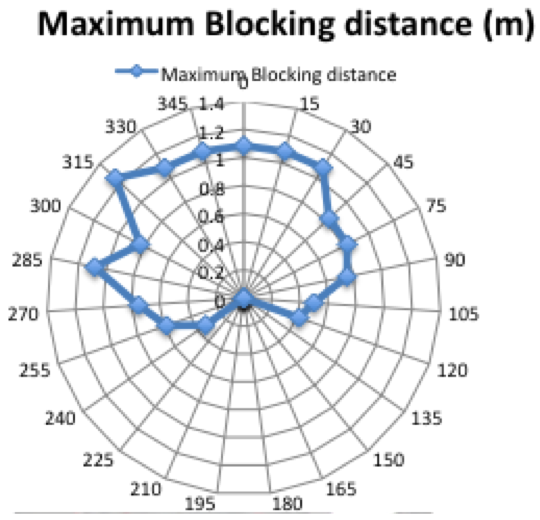

Fig. 14. Blocking Envelope Around Human Body.

In addition to the empirical results, we performed detailed electromagnetic simulations using simple human body models in the FEKO environment. FEKO simulations were done for a

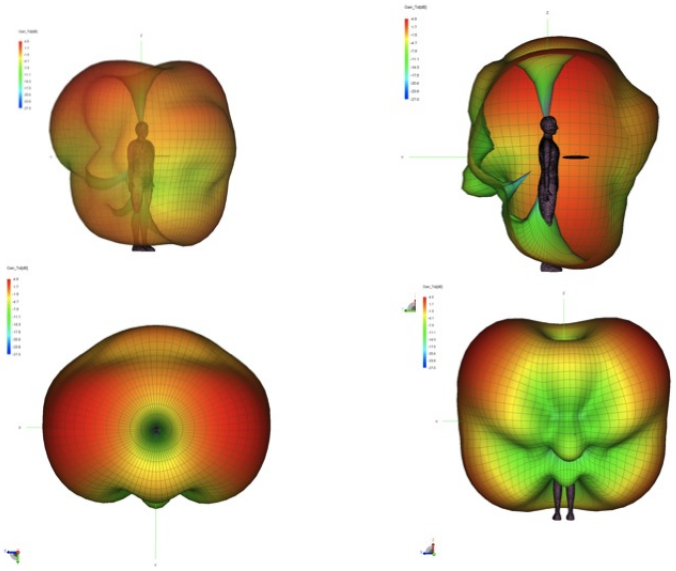

Fig. 15. FEKO Simulation of Monopole Antenna in Front of Human Body.

monopole antenna 30cm in front of the human body. Figure 15 shows the FEKO simulation results. The monopole antenna free space radiation pattern is very similar to a donut shape [8], but it is deformed due to the presence of human body [2].

The blocking envelope determined by the FEKO simulations are very similar to the blocking envelopes measured in practice.

VII. Conclusion

The Blocking Reader is a low-cost privacy preserving device that successfully prevents unauthorized reading of tags. The Blocking Reader creates a blocking envelope around itself that prevents tags within the envelope from being read by any unauthorized readers. The Blocking Reader can be used to ensure a person's privacy by simply carrying it as a person would carry a cell phone. Furthermore, the Blocking Reader uses the same protocol as the readers and tags, and it is designed to be FCC compliant. With more sophisticated turn-on intelligence and other reader detection functionality, a Blocking Reader can be integrated into a cellular telephone, turning the phone into an intrusion detection and privacy protection device.

For the experiments done in laboratory environment with power levels ranging from 19dBm to 21dBm radiated by a Blocking Reader, there is a maximum blocking distance of 1.3m. For power levels from 6dBm to 9dBm the maximum blocking distance is observed to be 1m. Therefore, a Blocking Reader can provide a good blocking of unauthorized tag reads with a controllable blocking envelope. Also, for the experiments done in the laboratory environment with a human body, we see that the Blocking Reader will create a secure blocking envelope of about 1m around the person, even on the opposite side of the human from the Blocking Reader. This envelope successfully blocks unauthorized readers trying to read the person's tags.

With the use of a simple low-cost Blocking Reader, the privacy of the RFID systems can be preserved. Our future research is focused upon making an Ultra-Low-Cost Reader with Blocking Reader capabilities and improved reader detection and security capabilities.

References

[1] Darmindra D Arumugam, Ananyaa Gautham, Gaurov Narayanaswamy, Nikhil Ayer, and Daniel W Engels. Impact of Human Presence on the Read Zones of Passive UHF RFID Systems. *International Journal on Radio Frequency Identification Technology and Applications*, 2(1/2):46–63, 2009.

[2] Dramindra D. Arumugam, Ananyaa Gautham, Gaurov Narayanaswamy, and Daniel W. Engels. Impact of RF Radiation on the Human Body in a Passive Wireless Healthcare Environment. *IEEE Conference on Ambient Pervasive Healthcare APiPH*, 2008.

[3] Manish Bhuptani and Shahrammoradpour. *RFID Field Guide: Deploying Radio Frequency Identification Systems*. Sun Microsystems Press, 2005.

[4] W.N. Cottingham and D.A. Greenwood. *Electricity and Magnetism*. Cambridge University Press, 1991.

[5] Daniel W. Engels. Review of rfid technology. *Texas RF Innovation and Technology Center*, 2007.

[6] Minoru Fujimoto. *Physics of Classical Electromagnetism*. Springer, 2007.

[7] R. Glidden. Design of ultra-low-cost uhf rfid tags for supply chain applications. *IEEE Communications Magazine*, 42:140–151, 2004.

[8] Lal Chand Godara. *Handbook of Antennas In Wireless Communications*. CRC Press LLC, 2002.

[9] EPC Global Inc. Epc global radio frequency identity air interface protocol class 1 generation 2 uhf rfid version 1.0.5, 2004.

[10] Texas Instruments. CC1101. http://focus.ti.com/lit/ds/symlink/cc1101.pdf.

[11] Ari Juels. Rfid security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication*, 24(2), February 2006.

[12] Ari Juels and Ravi Pappu. Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In R. Wright, editor, *Financial Cryptography '03*. Springer-Verlag., 2003.

[13] Ari Juels, Ronald L Rivest, and Michael Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. In *8th ACM Conference on Computer and Communications Security*, pages 103–111, 2003.

[14] Pavel Nikitin and KVS Rao. Theory and measurement of backscattering from rfid tags. *IEEE-Antennas and Propagation Magazine*, 48(6):212–218, 2006.

[15] M. Ohkubo, K. Suzuki, and S. Kinoshita. Rfid privacy issues and technical challenges. *ACM Commununication Journal*, 48(9):66–71, 2005.

[16] Daniel W. Engels Sanjay E. Sharma, Stephen A. Weis. Rfid systems. security and privacy implications. Technical report, MIT Auto-ID Center, February 2002.

[17] Tom Scharfeld. An analysis of fundamental constraint on low cost passive rfid system design. Master's thesis, Massachusetts Institute of Technology, 2001.

[18] Ronald Rivest Stephen A. Weis, Sanjay E. Sarma and Daniel W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *First International Conference on Security in Pervasive Computing*, 2003.

[19] L. Sydanheimol, J. Nummetla, L. Ukkonen, J. McVay, A. Hoorfar, and M. Kivikoskil. Characterization of passive UHF RFID tag performance. *IEEE Antennas and Propagation Magazine*, 50(3):207–212, 2008.

[20] Stephen A. Weis. Radio frequency identification security and privacy. Master's thesis, Massachusetts Institute of Technology, May 2003.

[21] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *Security in Pervasive Computing*, volume 2802 of *Lecture Notes in Computer Science*, pages 201–212. Springer, 2004.

[22] Markus Whn. *Electromagnetic Field Theory: A Problem Solving Approach*. John Wiley and Sons, 1999.